FIPS PUB *#HMAC*

FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION

The Keyed-Hash Message Authentication Code (HMAC)

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Issued MONTH DAY, 2001

U.S. Department of Commerce
Norman Y. Mineta, Secretary

Technology Administration
Cheryl L. Shavers, Under Secretary for Technology

National Institute of Standards and Technology
Raymond G. Kammer, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

William Mehuron, Director
Information Technology Laboratory

Abstract

This standard describes a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative FIPS-approved cryptographic hash function, in combination with a shared secret key. The cryptographic strength of HMAC depends on the properties of the underlying hash function. The HMAC specification in this standard is a generalization of Internet RFC 2104, *HMAC, Keyed-Hashing for Message Authentication*, and ANSI X9.71, *Keyed Hash Message Authentication Code*.

Keywords: computer security, cryptography, HMAC, MAC, message authentication, Federal Information Processing Standard (FIPS).

National Institute of Standards and Technology
FIPS PUB *#HMAC*
pages (MONTH DAY, 2001)
CODEN: XXXXX

U.S. Government Printing Office
Washington, 2000

For Sale by the National Technical Information Service
U.S. Department of Commerce
Springfield, VA 22161

Federal Information Processing Standards Publication *#HMAC*

2001 MONTH DAY

Announcing the Standard for

The Keyed-Hash Message Authentication Code (HMAC)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. **Name of Standard.** Keyed-Hash Message Authentication Code (HMAC) (FIPS PUB *#HMAC*).

2. **Category of Standard.** Computer Security Standard. **Subcategory.** Cryptography.

3. **Explanation.** This standard specifies an algorithm for applications requiring message authentication. Message authentication is achieved via the construction of a message authentication code (MAC). MACs based on cryptographic hash functions are known as HMACs.

The purpose of a MAC is to authenticate both the source of a message and its integrity without the use of any additional mechanisms. HMACs have two functionally distinct parameters, a message input and a secret key known only to the message originator and intended receiver(s). Additional applications of keyed hash functions include their use in challenge-response identification protocols for computing responses, which are a function of both a secret key and a challenge message.

An HMAC function is used by the message sender to produce a value (the MAC) that is formed by condensing the secret key and the message input. The MAC is typically sent to the message receiver along with the message. The receiver computes the MAC on the received message using the same key and HMAC function as was used by the sender, and compares the result computed with the received MAC. If the two values match, the message has been correctly received, and the receiver is assured that the sender is a member of the community of users that share the key.

The HMAC specification in this standard is a generalization of HMAC as specified in Internet RFC 2104, *HMAC, Keyed-Hashing for Message Authentication*, and ANSI X9.71, *Keyed Hash Message Authentication Code.*

4. **Approving Authority.** Secretary of Commerce.

5. Maintenance Agency. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

6. Applicability. This standard is applicable to all Federal departments and agencies for the protection of sensitive unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code. This standard shall be used in designing, acquiring and implementing message authentication in systems that Federal departments and agencies operate or which are operated for them under contract. The adoption and use of this standard is available to private and commercial organizations.

7. Specifications. Federal Information Processing Standard (FIPS) *#HMAC*, Keyed-Hash Message Authentication Code (HMAC) (affixed).

8. Implementations. Cryptographic modules that implement this standard shall conform to FIPS 140-1. The authentication mechanism described in this standard may be implemented in software, firmware, hardware, or any combination thereof. NIST has developed a Cryptographic Module Validation Program that will test implementations for conformance with this HMAC standard. Information on this program is available at http://csrc.nist.gov/cryptval/.

Agencies are advised that keys used for HMAC applications should not be used for other purposes.

9. Other Approved Security Functions. HMAC implementations that comply with this standard shall employ cryptographic algorithms, cryptographic key generation algorithms and key management techniques that have been approved for protecting Federal government sensitive information. Approved cryptographic algorithms and techniques include those that are either:

a. specified in a Federal Information Processing Standard (FIPS), or
b. adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

10. Export Control. Certain cryptographic devices and technical data regarding them are subject to Federal export controls and exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce. Applicable Federal government export controls are specified in Title 15, Code of Federal Regulations (CFR) Part 740.17; Title 15, CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.

11. Implementation Schedule. This standard becomes effective on [insert date: six months after approval by the Secretary of Commerce].

12. Qualifications. The security afforded by the HMAC function is dependent on maintaining the secrecy of the key. Users must therefore guard against disclosure of these

keys. While it is the intent of this standard to specify a mechanism to provide message authentication, conformance to this standard does not assure that a particular implementation is secure. It is the responsibility of the implementer to ensure that any module containing an HMAC implementation is designed and built in a secure manner.

Similarly, the use of a product containing an implementation that conforms to this standard does not guarantee the security of the overall system in which the product is used. The responsible authority in each agency shall assure that an overall system provides an acceptable level of security.

Since a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, this standard will be reviewed every five years in order to assess its adequacy.

13. Waiver Procedure. Under certain exceptional circumstances, the heads of Federal agencies, or their delegates, may approve waivers to Federal Information Processing Standards (FIPS). The heads of such agencies may redelegate such authority only to a senior official designated pursuant to Section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when compliance with this standard would

a. adversely affect the accomplishment of the mission of an operator of Federal computer system or

b. cause a major adverse financial impact on the operator that is not offset by government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision that explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decision, Information Technology Laboratory, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is

authorized and decides to make under Section 552(b) of Title 5, U.S. Code, shall be part of the procurement documentation and retained by the agency.

14. Where to obtain copies. This publication is available by accessing http://csrc.nist.gov/publications/. A list of other available computer security publications, including ordering information, can be obtained from NIST Publications List 91, which is available at the same web site. Alternatively, copies of NIST computer security publications are available from: National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161.

Federal Information Processing Standards Publication xxx

2000 *Month Day*

Specifications for

The Keyed-Hash Message Authentication Code

TABLE OF CONTENTS

1. INTRODUCTION

Providing a way to check the integrity of information transmitted over or stored in an unreliable medium is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity checks based on a secret key are usually called message authentication codes (MACs). Typically, message authentication codes are used between two parties that share a secret key in order to authenticate information transmitted between these parties. This standard defines a MAC that uses a cryptographic hash function in conjunction with a secret key. This mechanism is called HMAC and is a generalization of HMAC as specificatied in [RFC2104] and [ANSIX9.17].

HMAC shall be used in combination with a cryptographic hash function specified in a Federal Information Processing Standard (FIPS). HMAC uses a secret key for the calculation and verification of the MACs. The main goals behind the HMAC construction [RFC2104] are:

- To use available hash functions without modifications; in particular, hash functions that perform well in software, and for which code is freely and widely available,

- To preserve the original performance of the hash function without incurring a significant degradation,

- To use and handle keys in a simple way,

- To have a well-understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the underlying hash function, and

- To allow for easy replaceability of the underlying hash function in the event that faster or more secure hash functions are later available.

2. GLOSSARY OF TERMS AND ACRONYMS

2.1 Glossary of Terms

The following definitions are used throughout this standard:

FIPS-Approved: An algorithm or technique that is either 1) specified in a FIPS, or 2) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS..

Message Authentication Code (MAC): a cryptographic checksum that results from passing data through a message authentication algorithm. In this standard, the message authentication algorithm is called HMAC.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm. In this standard, the cryptographic key is used by the HMAC algorithm to produce a MAC on the data.

Keyed hash-based message authentication code (HMAC): a message authentication code that uses a cryptographic key in conjunction with a hash function.

Secret key: a cryptographic key that is uniquely associated with one or more entities. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.

2.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
HMAC	Keyed-Hash Message Authentication Code
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
SHA-1	The Secure Hash Algorithm specified in FIPS 180-1.

2.3 HMAC Parameters and Symbols

HMAC uses the following parameters:

B	Block size (in bytes) of the input to the FIPS-approved hash function; e.g., for SHA-1, *B* = 64.
H	FIPS-approved hash function, e.g., FIPS 180-1, *Secure Hash Algorithm-1 (SHA-1).*
ipad	Inner pad; the byte x’36’ repeated *B* times.
K	Secret key shared between the originator and the intended receiver(s).
K_0	The key *K* with zeros appended to form a *B* byte key.

L Block size (in bytes) of the output of the FIPS-approved hash function; for SHA-1, *L* = 20.

opad Outer pad; the byte x'5c' repeated *B* times.

t The number of bytes of MAC.

text The data on which the HMAC is calculated; the length of the data is *n* bits, where the maximum value for *n* depends on the hash algorithm used.

x'*N*' Hexadecimal notation, where each '*N*' represents 4 binary bits.

|| Concatenation

⊕ Exclusive-Or operation.

3. CRYPTOGRAPHIC KEYS

The size of the key, *K*, shall be equal to or greater than *L*/2, where *L* is the size of the hash function output. Note that keys greater than *L* bytes do not significantly increase the function strength. Applications that use keys longer than *B*-bytes shall first hash the key using *H* and then use the resultant *L*-byte string as the HMAC key, *K*. Keys shall be chosen at random using a FIPS-approved key generation method and shall be changed periodically. The keys shall be protected in a manner that is consistent with the value of the data that is to be protected (i.e., the data that is authenticated using the HMAC function).

4. TRUNCATED OUTPUT

A well-known practice with MACs is to truncate their output (i.e., the length of the MAC used is less than the length of the output of the MAC function *L*). Applications of this standard may truncate the output of HMAC. When a truncated HMAC is used, the *t* leftmost bytes of the HMAC computation shall be used as the MAC. The output length, *t*, shall be no less than four bytes (i.e., $4 \leq t \leq L$). However, *t* shall be at least $\frac{L}{2}$ bytes (i.e., $\frac{L}{2} \leq t \leq L$) unless an application or protocol makes numerous trials impractical. For example, a low bandwidth channel might prevent numerous trials on a 4 byte MAC, or a protocol might allow only a small number of invalid MAC attempts.

5. HMAC SPECIFICATION

To compute a MAC over the data '*text*' using the HMAC function, the following operation is performed:

$$\boldsymbol{MAC(text)_t = HMAC(K, text)_t = H((K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text))_t}$$

Table 1 illustrates the step by step process in the HMAC algorithm, which is depicted in Figure 1.

Table 1: The HMAC Algorithm

STEPS	STEP-BY-STEP DESCRIPTION
Step 1	If the length of $K = B$, set $K_0 = K$. Go to step 4.
Step 2	If the length of $K > B$, hash K to obtain an L byte string: $K = H(K)$.
Step 3	If the length of $K < B$, append zeros to the end of K to create a B-byte string K_0 (e.g., if K is 20 bytes in length and $B = 64$, then K will be appended with 44 zero bytes 0x00).
Step 4	Exclusive-Or K_0 with *ipad* to produce a B-byte string: $\boldsymbol{K_0 \oplus ipad}$.
Step 5	Append the stream of data '*text*' to the string resulting from step 4: $\boldsymbol{(K_0 \oplus ipad) \| text}$.
Step 6	Apply H to the stream generated in step 5: $\mathbf{H}(\boldsymbol{(K_0 \oplus ipad) \| text})$.
Step 7	Exclusive-Or K_0 with *opad*: $\boldsymbol{K_0 \oplus opad}$.
Step 8	Append the result from step 6 to step 7: $\boldsymbol{(K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text)}$.
Step 9	Apply H to the result from step 8: $\boldsymbol{H((K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text))}$.
Step 10	Select the leftmost t bytes of the result of step 9 as the MAC.

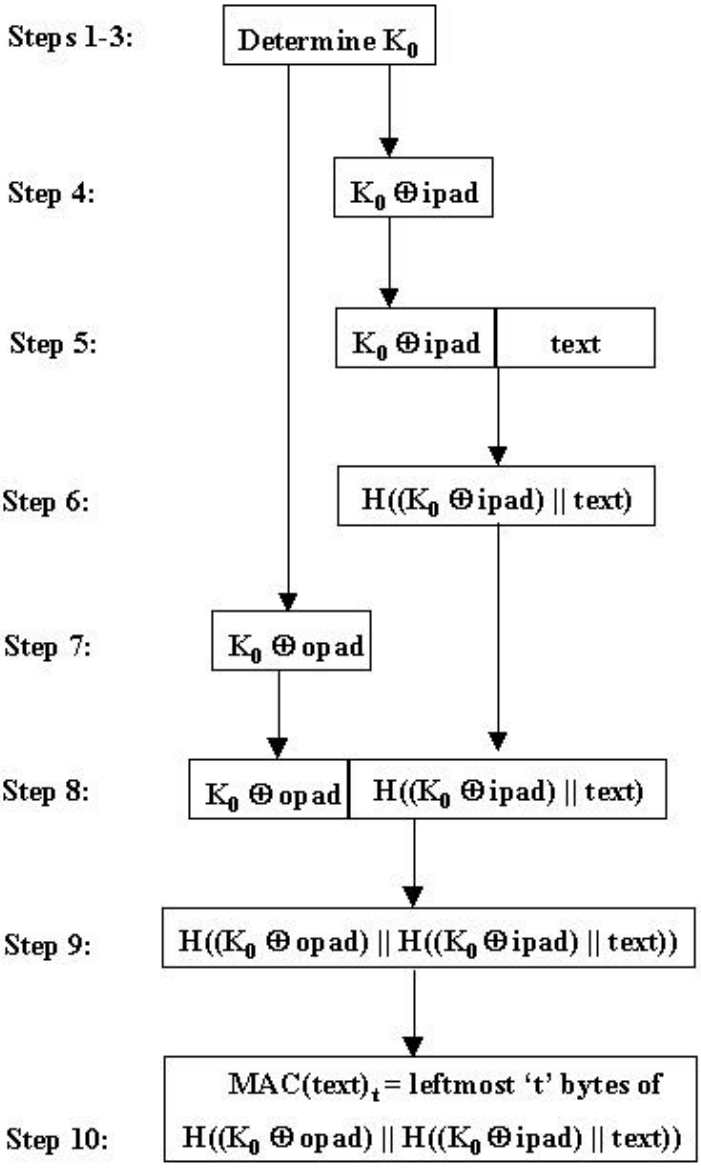

Figure 1: Illustration of the HMAC Construction

6. IMPLEMENTATION NOTE

The HMAC algorithm is specified for an arbitrary FIPS-approved cryptographic hash function, *H*. With minor modifications, an HMAC implementation can easily replace one hash function, *H*, with another hash function, *H'*.

Conceptually, the intermediate results of the compression function on the *B*-byte blocks ($K_0 \oplus ipad$) and ($K_0 \oplus opad$) can be precomputed once, at the time of generation of the

key *K*, or before its first use. These intermediate results can be stored and then used to initialize *H* each time that a message needs to be authenticated using the same key. For each authenticated message using the key *K*, this method saves the application of the hash function of *H* on two *B*-byte blocks (i.e., on ($K \oplus ipad$) and ($K \oplus opad$)). This saving may be significant when authenticating short streams of data. **These stored intermediate values shall be treated and protected in the same manner as secret keys.**

Choosing to implement HMAC in this manner has no effect on interoperability.

APPENDIX A: HMAC EXAMPLES

These examples are provided in order to promote correct implementations of HMAC.

A.1 SHA-1 Examples: B = 64 bytes; L = 20 bytes

[NOTE: These examples were taken from ANSI X9.71]

Test case 1 (20 byte key; 20 byte HMAC)**:**

key = x’0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b’

data = "Hi There"

HMAC = x’b617318655057264e28bc0b6fb378c8ef146be00’

Test case 2 (20 byte key; 20 byte HMAC):

key = x’aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa’

data = x’dd’ repeated 50 times

HMAC = x’125d7342b9ac11cd91a39af48aa17b4f63f175d3’

Test case 3 (25 byte key; 20 byte HMAC):

key = x’0102030405060708090a0b0c0d0e0f10111213141516171819’

data = x’cd’ repeated 50 times

HMAC = x’4c9007f4026250c6bc8414f9bf50c86c2d7235da’

Test case 4 (20 byte key; 20 byte MAC; 12 byte MAC):

key = x’0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c0c’

data = "Test With Truncation"

HMAC = x’4c1a03424b55e07fe7f27be1d58bb9324a9a5a04’

96-bit MAC = x’4c1a03424b55e07fe7f27be1’

APPENDIX B: REFERENCES

[ANSIX9.71] American Bankers Association, *Keyed Hash Message Authentication Code,* ANSI X9.71, Washington, D.C., 2000.

[FIPS113] National Institute of Standards and Technology, *Computer Data Authentication,* Federal Information Processing Standards Publication 113, 30 May 1985.

[FIPS140-2] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules,* Federal Information Processing Standards Publication 140-2, DD Month 2000.

[FIPS171] National Institute of Standards and Technology, *Key Management Using ANSI X9.17,* Federal Information Processing Standards Publication 171, 27 April 1992.

[FIPS180-1] National Institute of Standards and Technology, *Secure Hash Standard (SHS),* Federal Information Processing Standards Publication 180-1, 17 April 1995.

[ISO9797-2] Joint Technical Committee ISO/IEC JTC 1 Subcommittee SC 27, *Information technology – Security techniques – Message authentication codes (MACs) – Part 2: Mechanisms using a hash-function,* ISO/IEC FCD 9797-2, 15 July 1999.

[RFC2104] H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication,* Internet Engineering Task Force, Request for Comments (RFC) 2104, February 1997.

[RFC2404] C. Madson and R. Glenn, *The Use of HMAC-SHA-1-96 within ESP and AH,* Internet Engineering Task Force, Request for Comments (RFC) 2404, November 1998.